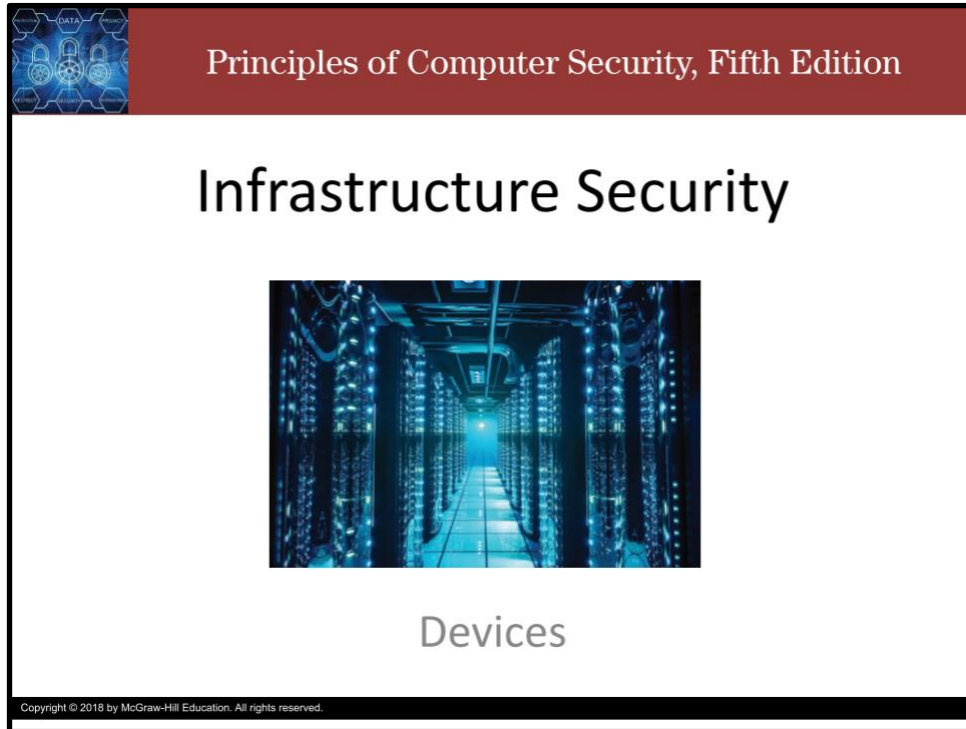


Infrastructure Security: Devices


Slide 1



The image shows the cover of a book titled "Principles of Computer Security, Fifth Edition". The cover has a dark red header with the title in white. Below the header, the main title "Infrastructure Security" is written in a large, black, sans-serif font. Underneath the title is a photograph of a server room with rows of server racks illuminated by blue lights. Below the photograph, the word "Devices" is written in a smaller, grey, sans-serif font. In the top left corner of the cover, there is a small graphic with the word "DATA" and several padlock icons. At the bottom of the cover, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy! In this video, we introduce some of the devices that make up a network's infrastructure.

Slide 2



Principles of Computer Security, Fifth Edition

Devices

- Devices are needed to connect clients and servers and to regulate the traffic between them.
- Devices expand the network beyond simple client computers and servers.
- Devices come in many forms and with many functions.
- Each device has a specific network function and plays a role in maintaining network infrastructure security.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Devices are needed to connect clients and servers and to regulate the traffic between them.


But, a complete network solution in today's business environment consists of more than just client computers and servers.

Devices are also needed to expand a network beyond simple client computers and servers to include other devices, such as wireless and handheld systems.

Devices come in many forms and with many functions, from hubs and switches, to routers, wireless access points, and special-purpose devices like VPN connectors.

Each device has a specific network function and plays a role in maintaining network infrastructure security.

Slide 3



Principles of Computer Security, Fifth Edition

Workstations

- The **workstation** is the machine that sits on the desktop.
 - Used every day for various activities
 - Important part of the network security solution.
 - Many threats to information security can start at a workstation
 - Much can be done in a few simple steps to provide protection from many of these threats.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Most users are familiar with the client computers used in the client/server model called **workstation** devices.


The **workstation** is the machine that sits on the desktop.

It is used every day for sending and reading e-mail, creating spreadsheets, writing reports in a word processing program, and playing games.

A workstation connected to a network is an important part of the network security solution.

Many threats to information security can start at a workstation, but much can be done in a few simple steps to provide protection from many of these threats.

Slide 4



Principles of Computer Security, Fifth Edition

Servers

- **Servers** are the computers in a network that host applications and data for everyone to share.
 - Servers come in many sizes.
- Server operating systems range from Windows Server, to UNIX, to Multiple Virtual Storage (MVS) and other mainframe operating systems
 - They tend to be more robust than workstation OSs.
 - They are designed to service multiple users over a network at the same time.
- Servers can host a variety of applications.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Servers are the computers in a network that host applications and data for everyone to share.


Servers come in many sizes, from small single-CPU boxes that may be less powerful than a workstation, to multiple-CPU monsters, up to and including mainframes.

The operating systems used by servers range from Windows Server to UNIX, to Multiple Virtual Storage (MVS) and other mainframe operating systems.

The OS on a server tends to be more robust than the OS on a workstation system and is designed to service multiple users over a network at the same time.

Servers can host a variety of applications, including web servers, databases, e-mail servers, file servers, print servers, and application servers for middleware applications.

Slide 5



Principles of Computer Security, Fifth Edition

Mobile Devices


- Mobile devices such as laptops, tablets, and mobile phones are the latest devices to join the corporate network.
- Mobile devices can create a major security gap, as a user may access separate e-mail accounts, one personal, without antivirus protection, and the other corporate.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Mobile devices such laptops, tablets, and mobile phones are just the latest devices to join the corporate network.

Mobile devices can create a major security gap, as a user may access separate e-mail accounts, one personal, without antivirus protection, and the other corporate.

Slide 6




Principles of Computer Security, Fifth Edition

Device Security, Common Concerns

- As more and more interactive devices are being designed, a new threat source has appeared.
- Default accounts and passwords are well known in the hacker community.
 - First steps you must take to secure such devices is to change the default credentials.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

In an attempt to build security into devices, typically, a default account and password must be entered to enable the user to access and configure the device remotely. These default accounts and passwords are well known in the hacker community, so one of the first steps you must take to secure such devices is to change the default credentials. Anyone who has purchased a home office router knows the default configuration settings and can check to see if another user has changed theirs. If they have not, this is a huge security hole, allowing outsiders to “reconfigure” their network devices.



Principles of Computer Security, Fifth Edition

Network-Attached Storage

- Because of the speed of today's Ethernet networks, it is possible to manage data storage across the network.
- This has led to a type of storage known as **Network-Attached Storage (NAS)**.
 - The combination of inexpensive hard drives, fast networks, and simple application-based servers has made NAS devices in the terabyte range affordable for even home users.
- As a network device, it is susceptible to attacks.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Because of the speed of today's Ethernet networks, it is possible to manage data storage across the network.

This has led to a type of storage known as **Network- Attached Storage or NAS**.

The combination of inexpensive hard drives, fast networks, and simple application-based servers has made NAS devices in the terabyte range affordable for even home users.

Because of the large size of video files, this has become popular for some users as a method of storing TV and video libraries. Because **NAS** is a network device, it is susceptible to various attacks, including sniffing of credentials and a variety of brute-force attacks to obtain access to the data.



Removable Storage

- Removable devices can move data outside of the corporate-controlled environment.
- Removable devices can bring unprotected or corrupted data into the corporate environment.
- All removable devices should be scanned by antivirus software upon connection to the corporate environment.
- Corporate policies should address the copying of data to removable devices.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Many mobile devices can be connected via USB to a system and used to store data—and in some cases vast quantities of data.

This capability can be used to circumvent some implementations of data loss prevention mechanisms.

Not only can removable devices (like a smart phone or a USB flash drive) move data outside of the corporate-controlled environment,

they can also bring unprotected or corrupted data into the environment.

All removable devices should be scanned by antivirus software upon connection.

Additionally, corporate policies should address the copying of data to removable devices. To be effective, those policies need some mechanism for enforcement.

Slide 9



Principles of Computer Security, Fifth Edition

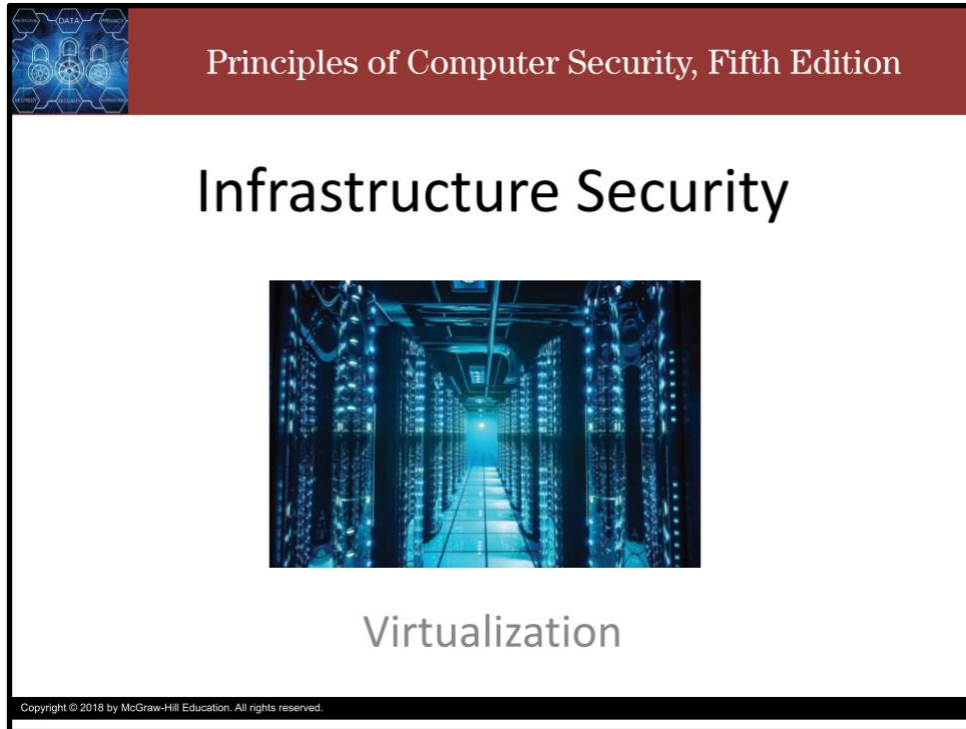
Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Thank you and take care.


Infrastructure Security: Virtualization

Slide 1



Principles of Computer Security, Fifth Edition

Infrastructure Security




Virtualization

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss virtualization.

Slide 2



Principles of Computer Security, Fifth Edition

Virtualization

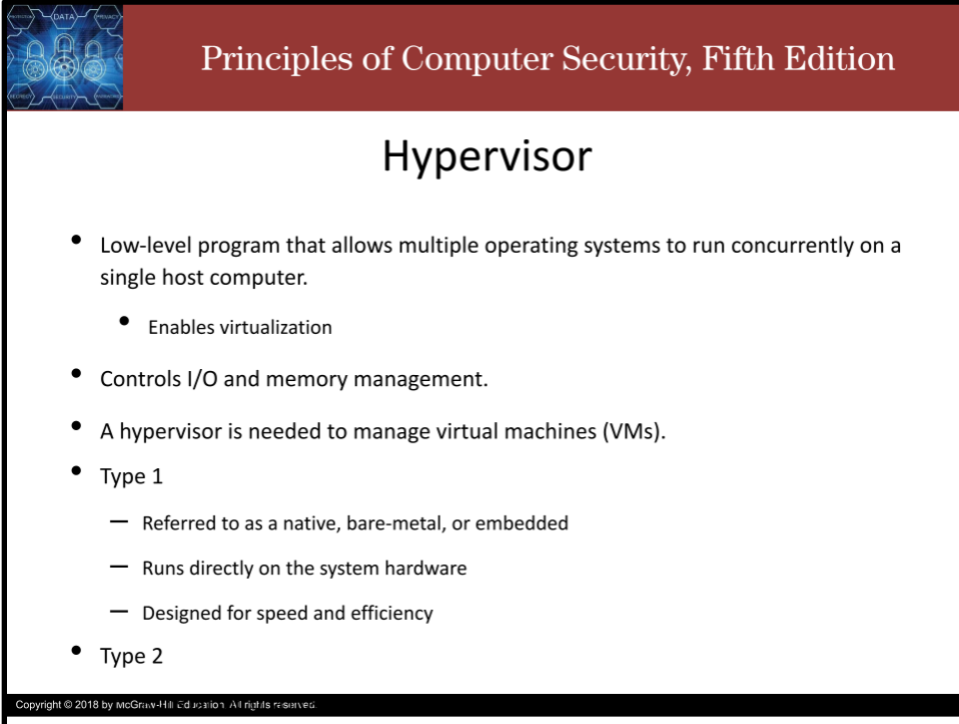
- Virtualization technology is used to allow a computer to have more than one OS present and, in many cases, operating at the same time.
- **Virtualization** is an abstraction of the OS layer.
 - It creates the ability to host multiple OSs on a single piece of hardware.
- A major advantage of virtualization is the separation of the software and the hardware.
 - It creates a barrier that can improve many system functions, including security.
- The underlying hardware is referred to as the host machine, and on it is a host OS.
 - Virtual machines are typically referred to as the guest OSs.
- Newer OSs are designed to natively incorporate virtualization hooks.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Virtualization technology is used to allow a computer to have more than one OS present and, in many cases, operating at the same time. **Virtualization** is an abstraction of the OS layer which creates the ability to host multiple OSs on a single piece of hardware. A major advantage of virtualization is the separation of the software and the hardware. It creates a barrier that can improve many system functions, including security.

The underlying hardware is referred to as the host machine, and on it is a host OS. Virtual machines are typically referred to as the guest OSs. Newer OSs are designed to natively incorporate virtualization hooks, enabling virtual machines to be employed with greater ease. Common virtualization solutions include VMware, VirtualBox, Parallels, and Zen

Slide 3



Principles of Computer Security, Fifth Edition

Hypervisor

- Low-level program that allows multiple operating systems to run concurrently on a single host computer.
 - Enables virtualization
- Controls I/O and memory management.
- A hypervisor is needed to manage virtual machines (VMs).
- Type 1
 - Referred to as a native, bare-metal, or embedded
 - Runs directly on the system hardware
 - Designed for speed and efficiency
- Type 2

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A hypervisor is the interface between a virtual machine and the host machine hardware. It is a low-level program that allows multiple operating systems to run concurrently on a single host computer.

It is the **hypervisor** that enables virtualization.

The hypervisor acts as the traffic cop that controls I/O and memory management.

Either the host OS has built-in hypervisor capability or an application is needed to provide the hypervisor function to manage the virtual machines

There are 2 types of hypervisors.

Referred to as a native, bare-metal, or embedded hypervisors, Type 1 hypervisors run directly on the system hardware.


They are designed for speed and efficiency, as they do not have to operate through another OS layer.

Type 2 hypervisors run on top of a host operating system.

In the beginning, Type 2 hypervisors were the most popular.

Typical Type 2 hypervisors include VirtualBox and VMware. This type of hypervisor is designed for limited numbers of VMs, typically in a desktop or small server environment.

Slide 4



Principles of Computer Security, Fifth Edition

Containers

- Containers holds the portions of an OS that it needs separate from the kernel.
- Multiple containers can share an OS and have separate memory, CPU, and storage threads.
- A container consists of an entire runtime environment
- Containers abstract away differences in underlying infrastructure.
- Example: Docker

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

In a hyper-visor-based virtualization system, multiple Oses can exist on a single hardware platform. Containers are the same idea, but rather than having multiple independent Oses, containers holds the portions of an OS that it needs separate from the kernel.


Multiple containers can share an OS and have separate memory, CPU, and storage threads.

This allows multiple instances of the application, or different applications, to share a host OS with virtually no overhead.

A container consists of an entire runtime environment – the application, plus all the dependencies, libraries and other binaries and configuration files needed to run it, all bundled into one reproducible package.

Because the application platform, including its dependencies, is containerized, any differences in OS distributions, libraries, and underlying infrastructure are abstracted away.

Slide 5



Principles of Computer Security, Fifth Edition

VM Sprawl Avoidance


- Sprawl is the uncontrolled spreading of disorganization caused by a lack of an organizational structure when many similar elements require management.
- VM sprawl is a symptom of a disorganized structure.
- VM sprawl avoidance needs to be implemented via policy and mechanism.
 - Use naming conventions and proper storage architecture

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Sprawl is the uncontrolled spreading of disorganization caused by a lack of an organizational structure when many similar elements require management.

VM sprawl is a symptom of a disorganized structure. VM sprawl avoidance is a real thing and needs to be implemented via policy and mechanism. You can fight VM sprawl by using naming conventions and proper storage architectures to make finding a specific VM easy and efficient.

Slide 6



Principles of Computer Security, Fifth Edition


VM Sprawl Avoidance

- Sprawl is the uncontrolled spreading of disorganization caused by a lack of an organizational structure when many similar elements require management.
- VM sprawl is a symptom of a disorganized structure.
- VM sprawl avoidance needs to be implemented via policy and mechanism.
 - Use naming conventions and proper storage architecture

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

VM escape occurs when software (typically malware) or an attacker escapes from a VM into the underlying OS. From there the attacker can pivot to attack the infrastructure or can move into other VMs. Large-scale VM environments have specific modules designed to detect escape and provide VM escape protection to other modules.

Slide 7



Principles of Computer Security, Fifth Edition


Snapshots

- A snapshot is a point-in-time saving of the state of a virtual machine.
- Snapshot uses:
 - Roll a system back to a previous point in time
 - Undo operations
 - Provide a quick means of recovery from a complex, system-altering change that has gone awry
- Snapshots act as a form of backup and are typically much faster than normal system backup and recovery operations.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A snapshot is a copy of the state of a VM at a single point-in-time. Snapshots can be used to roll a system back to a previous point in time, undo operations, or provide a quick means of recovery from a complex, system-altering change that has gone awry. Snapshots act as a form of backup and are typically much faster than normal system backup and recovery operations.

Slide 8




Principles of Computer Security, Fifth Edition

Patch Compatibility

- Patches are still needed and should be applied, independent of the virtualization status.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Just because it's in a VM, doesn't mean it's immune from attack or doesn't need to be updated. Patches are still needed and should be applied, independent of the virtualization status.



Principles of Computer Security, Fifth Edition

Host Availability/Elasticity


- In a virtualization environment, protecting the host OS and hypervisor level is critical for system stability.
- Best practice is to avoid the installation of any applications on the host-level machine.
- Elasticity refers to the ability of a system to expand/contract as system requirements dictate.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

In a virtualization environment, protecting the host OS and hypervisor level is critical for system stability. Best practice is to avoid the installation of any applications, other than the hypervisor, on the host-level machine.

Elasticity refers to the ability of a system to expand/contract as system requirements dictate. VMs can be moved between hardware to scale the available resource, like compute power and storage.

Slide 10



Principles of Computer Security, Fifth Edition

Security Control Testing


- It is important to test the controls applied to a system to manage security operations to ensure that they are providing the desired results.
- It is essential to specifically test all security controls inside the virtual environment to ensure their behavior is still effective.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

It is important to test the controls applied to a system to manage security operations to ensure that they are providing the desired results.

Putting a system into a VM does not exempt the system from this requirement.

It is essential to specifically test all security controls inside the virtual environment to ensure their behavior is still effective.



Principles of Computer Security, Fifth Edition


Sandboxing

- **Sandboxing** refers to the quarantine or isolation of a system from its surroundings.
- Virtualization can be used as a form of sandboxing with respect to an entire system.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Sandboxing refers to the quarantine or isolation of a system from its surroundings. Whatever happens in the sandbox, stays in the sandbox. Virtualization can be used as a form of sandboxing with respect to an entire system.

Slide 12



Principles of Computer Security, Fifth Edition

Attribution

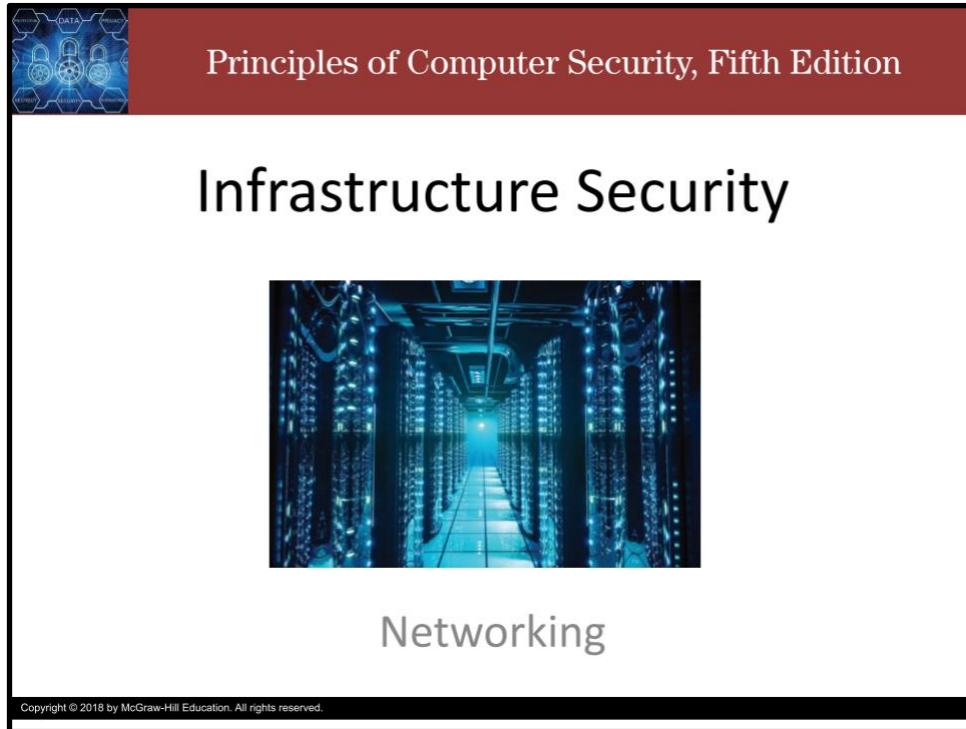
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Infrastructure Security: Networking


Slide 1



The image shows the cover of a book titled "Principles of Computer Security, Fifth Edition". The cover has a dark red header with the title in white. Below the header, the main title "Infrastructure Security" is written in a large, black, sans-serif font. Underneath the title is a photograph of a server room with rows of server racks illuminated by blue light. Below the photograph, the word "Networking" is written in a smaller, grey, sans-serif font. In the top left corner of the cover, there is a small graphic with the word "DATA" and several padlock icons. At the bottom of the cover, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Infrastructure Security




Networking

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, introduce some networking devices.

Slide 2



Principles of Computer Security, Fifth Edition

Networking

- Networks are used to connect devices together.
- Networks are composed of components that perform networking functions to move data between devices.
- Networks begin with network interface cards, then continue in layers of switches and routers.
- Specialized networking devices are used for specific purposes, such as security and traffic management.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Networks are used to connect devices together. They are composed of components that perform networking functions to move data between devices. Device-wise, the network starts at the network interface cards, and then continues in layers of switches and routers. There are specialized networking devices that are used for specific purposes, such as security and traffic management.

Slide 3

Principles of Computer Security, Fifth Edition

Network Interface Cards



Copyright © 2018 by McGraw-Hill Education. All rights reserved.

To connect a server or workstation to a network, a device known as a **network interface card (NIC)** is used. A **Network interface card** is a card with a connector port for a particular type of network connection, either Ethernet or Token Ring. The most common network type in use for LANs is the Ethernet protocol, and the most common connector is the RJ-45 connector. The purpose of a NIC is to provide lower-level protocol functionality from the OSI (Open System Interconnection) model. Because the NIC defines the type of physical layer connection, different NICs are used for different physical protocols. NICs come as single-port and multiport, and most workstations use only a single-port NIC, as only a single network connection is needed. For servers, multiport NICs are used to increase the number of network connections, increasing the data throughput to and from the network.

Each NIC port is serialized with a unique code, 48 bits long, referred to as a Media Access Control address (MAC address). These are created by the manufacturer, with 24 bits representing the manufacturer and 24 bits being a serial number, guaranteeing uniqueness. MAC addresses are used in the addressing and delivery of network packets to the correct machine and in a variety of security situations. Unfortunately, these addresses can be changed, or “spoofed,” rather easily. In fact, it is common for personal routers to clone a MAC address to allow users to use multiple devices over a network connection that expects a single MAC.

Slide 4



A **switch** forms the basis for connections in most Ethernet-based LANs.

Switches operate at the data link layer, while routers act at the network layer. For intranets, switches have become what routers are on the Internet—the device of choice for connecting machines. As switches have become the primary network connectivity device, additional functionality has been added to them. A switch is usually a Layer 2 (or data link layer) device, meaning that it makes its routing decisions based on the MAC address. Layer-3 (or network layer) switches can see the IP addresses and use the destination IP address to help make the routing decision. There are even layer-4 (or transport layer) switches that can read port numbers in order to route traffic based on the type of the traffic, like HTTP versus FTP.

Switches have important advantages over earlier devices like hubs and bridges.

A switch can improve network performance by only sending the data to the port on the switch that the destination system resides on. The switch knows what port each system is connected to and sends the data only to that port.

Switches also provide the option to disable a port so that it cannot be used without authorization.

Because switches are intelligent network devices, they can be targeted by attackers.

Should a hacker break into a switch and change its parameters, they might be able to eavesdrop on specific or all communications, virtually undetected.

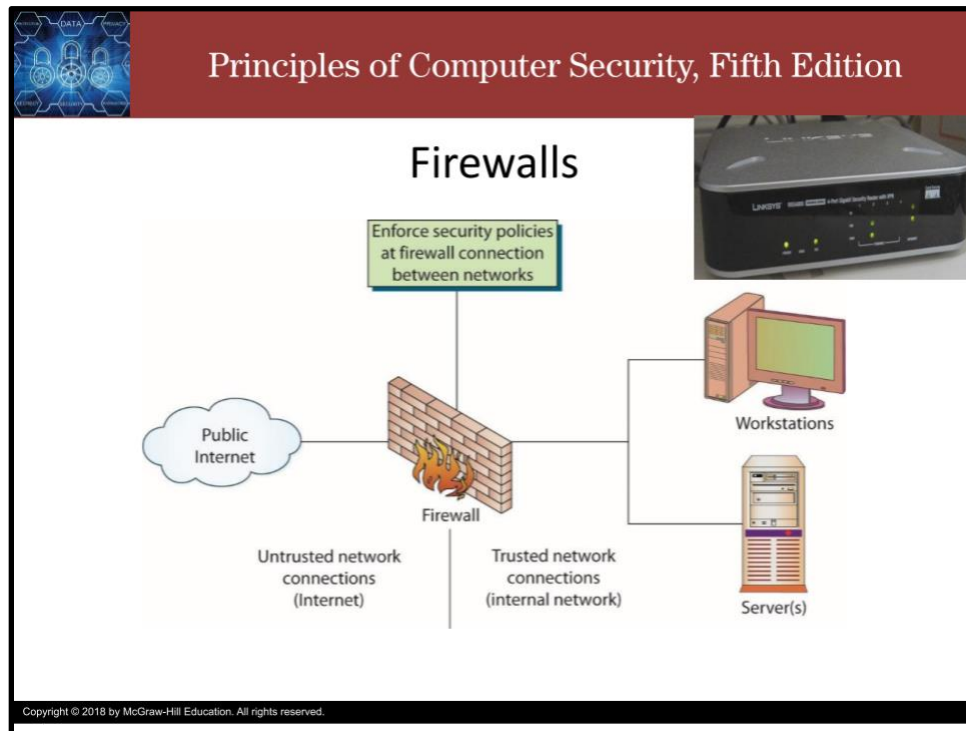
Switches are commonly administered using the Simple Network Management Protocol (SNMP) and Telnet protocol, both of which have a serious weakness in that they send passwords across the network in cleartext. A hacker armed with a sniffer that observes maintenance on a switch can capture the administrative password.

packets according to rules built into the ACLs. This can be a cumbersome process to set up and maintain, and as the access control lists grows in size, routing efficiency can be decreased. It is also possible to configure some routers to act as quasi-application gateways, performing stateful packet inspection and using contents as well as IP addresses to determine whether or not to permit a packet to pass. This can tremendously increase the time for a router to pass traffic and can significantly decrease router throughput. Configuring access control lists and other aspects of setting up routers for this type of use are beyond the scope of this module. One serious security concern regarding router operation is limiting who has access to the router and control of its internal functions. Like a switch, a router can be accessed using SNMP and Telnet and programmed remotely. Because of the geographic separation of routers, this can become a necessity, for many routers in the world of the Internet can be hundreds of miles apart, in separate locked structures. Physical control over a router is absolutely necessary, for if any device, be it a server, switch, or router, is physically accessed by a hacker, it should be considered compromised. Thus, such access must be prevented. As with switches, it is important to ensure that the administrator password is never passed in the clear, that only secure mechanisms are used to access the router, and that all of the default passwords are reset to strong passwords.

As with switches, the most assured point of access for router management control is via a direct physical connection. This allows access to the control aspects of the router without having to deal with traffic-related issues. For internal company networks, where the geographic dispersion of routers may be limited, third-party solutions to allow out-of-band remote management exist. This allows complete control over the router in a secure fashion, even from a remote location, although additional hardware is required.

Routers are available from numerous vendors and come in sizes big and small. A typical small home office router for use with cable modem/DSL service is shown in this figure on the left. Larger routers, like the one on the right, can handle traffic of up to tens of gigabytes per second per channel, using fiberoptic inputs and moving tens of thousands of concurrent Internet connections across the network. These routers, which can cost hundreds of thousands of dollars, form an essential part of e-commerce infrastructure, enabling large enterprises such as Amazon and eBay to serve many customers' use concurrently.

Slide 6



A **firewall** is a network device that enforces a security policy across its connections by allowing or denying traffic to pass into or out of the network.

A firewall is like a gate guard at a secure facility. The guard examines all the traffic trying to enter the facility—cars with the correct sticker or delivery trucks with the appropriate paperwork are allowed in; everyone else is turned away.

The heart of a **firewall** is the set of security policies that it enforces. Management determines what is allowed in the form of network traffic between devices, and these policies are used to build rule sets for the firewall devices used to filter network traffic across the network.

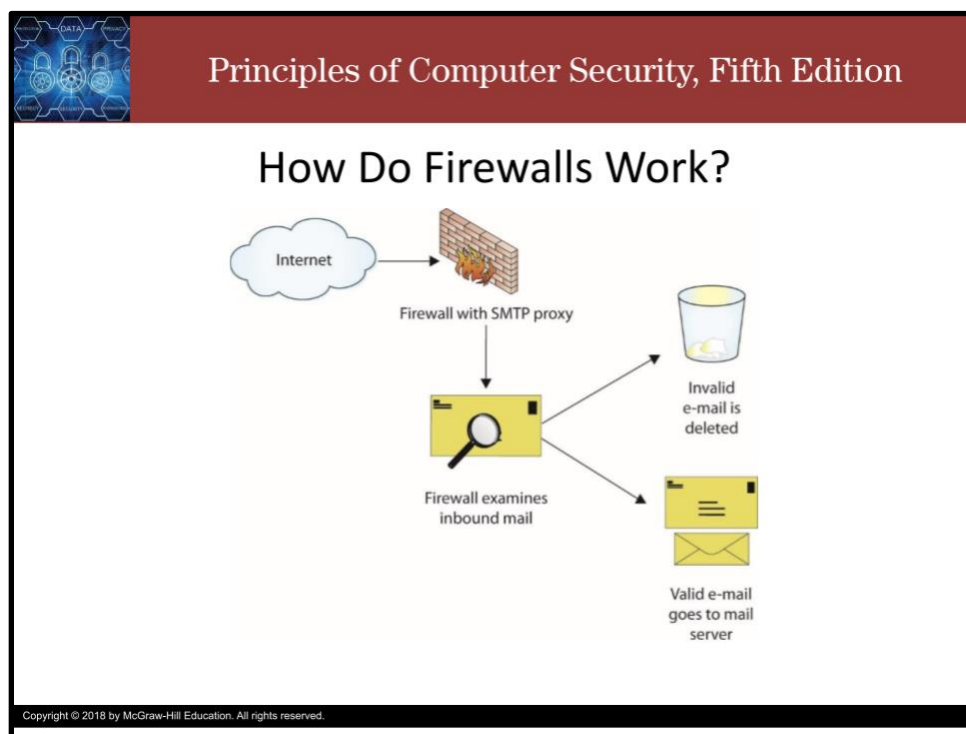
Firewall security policies are a series of rules that defines what traffic is permissible and what traffic is to be blocked or denied. These are not universal rules, and there are many different sets of rules for a single company with multiple connections. A web server connected to the Internet may be configured only to allow traffic on port 80 for HTTP, and have all other ports blocked. An e-mail server may have only necessary ports for e-mail open, with others blocked. Firewalls employ the principles of least privilege and economy of mechanism: Only allow the necessary access for a function; block or deny all unneeded functionality. How an organization deploys its firewalls determines what security policies are enforced by each firewall.

The perfect firewall policy is one that the end user never sees and one that never allows even a single unauthorized packet to enter the network. As with any other perfect item, it will be rare to find the perfect security policy for a firewall.

To develop a complete and comprehensive security policy, it is first necessary to have a complete and comprehensive understanding of your network resources and their uses. Once you know what your network will be used for, you will have an idea of what to permit. Also, once you understand what you need to protect, you will have an idea of what to block. Firewalls are designed to block attacks before they get to a target machine. Common targets are web servers, e-mail servers, DNS servers, FTP services, and databases. Each of these has separate functionality, and each of these has separate vulnerabilities. Once you have decided who should receive what type of traffic and what types should be blocked, you can administer this through the firewall.

At a minimum, the corporate connection to the Internet should pass through a firewall, as shown in this figure. This firewall should block all network traffic except that specifically authorized by the security policy. This is actually easy to do: blocking communications on a port is simply a matter of telling the firewall to close the port. The issue comes in deciding what services are needed and by whom, and thus which ports should be open and which should be closed. This is what makes a security policy useful but, in some cases, difficult to maintain.

Slide 7



Firewalls enforce the established security policies through a variety of mechanisms, including: Network Address Translation, Packet filtering, Access control lists, and Application layer proxies

As they are in routers, switches, servers, and other network devices, ACLs are a cornerstone of security in firewalls. Just as you must protect the device from physical access, ACLs do the same task for electronic access. Firewalls can extend the concept of ACLs by enforcing them at a packet level when


packet-level stateful filtering is performed. This can add an extra layer of protection, making it more difficult for an outside hacker to breach a firewall.

Firewalls can also act as network traffic regulators in that they can be configured to mitigate specific types of network-based attacks. In denial-of-service attacks, an attacker can attempt to flood a network with traffic. Firewalls can be tuned to detect these types of attacks and act as flood guards, mitigating the effect on the network.

Some high-security firewalls also employ application layer proxies. As the name implies, packets are not allowed to traverse the firewall, but data instead flows up to an application that in turn decides what to do with it. For example, an SMTP proxy may accept inbound mail from the Internet and forward it to the internal corporate mail server, as depicted in this figure.


While proxies provide a high level of security by making it very difficult for an attacker to manipulate the actual packets arriving at the destination, and while they provide the opportunity for an application to interpret the data prior to forwarding it to the destination, they generally are not capable of the same throughput as stateful packet-inspection firewalls. The trade-off between performance and speed is a common one and must be evaluated with respect to security needs and performance requirements.

Slide 8



Principles of Computer Security, Fifth Edition

Wireless Devices



A typical wireless access point

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Wireless devices bring additional security concerns.

Wireless network links use radio waves to carry data, which allows anyone within range access to the data.

Placing a wireless device behind a firewall does not do any good, because the firewall stops only physically connected traffic from reaching the device. Outside traffic can come literally from the parking lot directly to the wireless device and into the network.

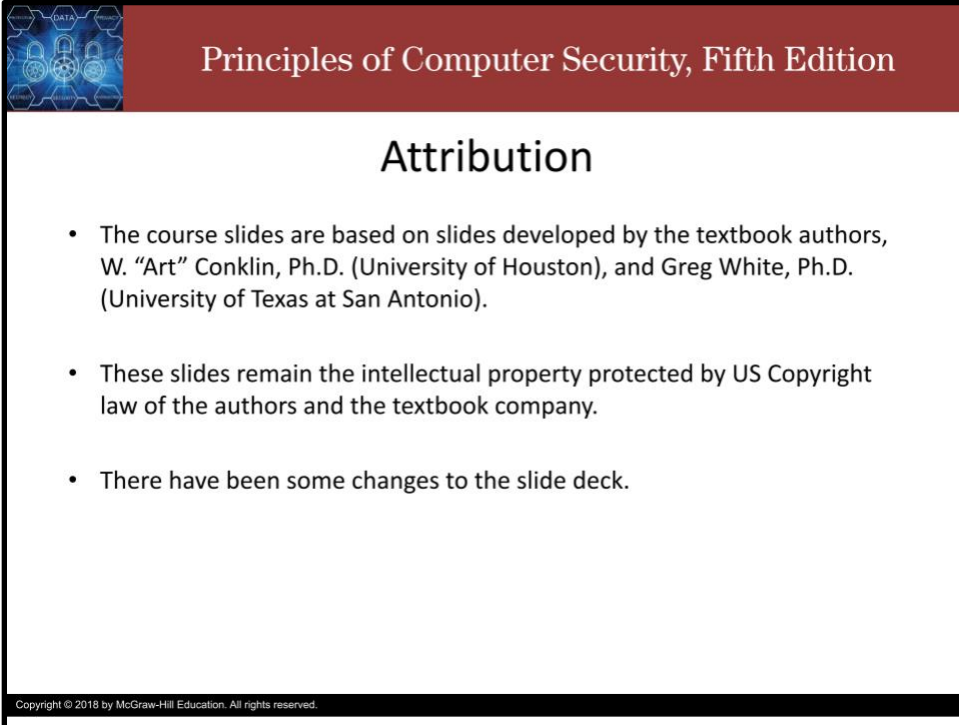
The point of entry from a wireless device to a wired network is performed at a device called a **wireless access point**.

Wireless access points can support multiple concurrent devices accessing network resources through the network node they create.

In the home or office, we colloquially refer to these as routers, or wireless routers.

Wireless access points and network interface cards must be matched by protocol for proper operation.

Slide 9



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the word "Attribution" is centered in a large, bold, black font. A bulleted list follows, containing three items. The slide is framed by a black border. In the bottom left corner, there is a small copyright notice.

Principles of Computer Security, Fifth Edition

Attribution

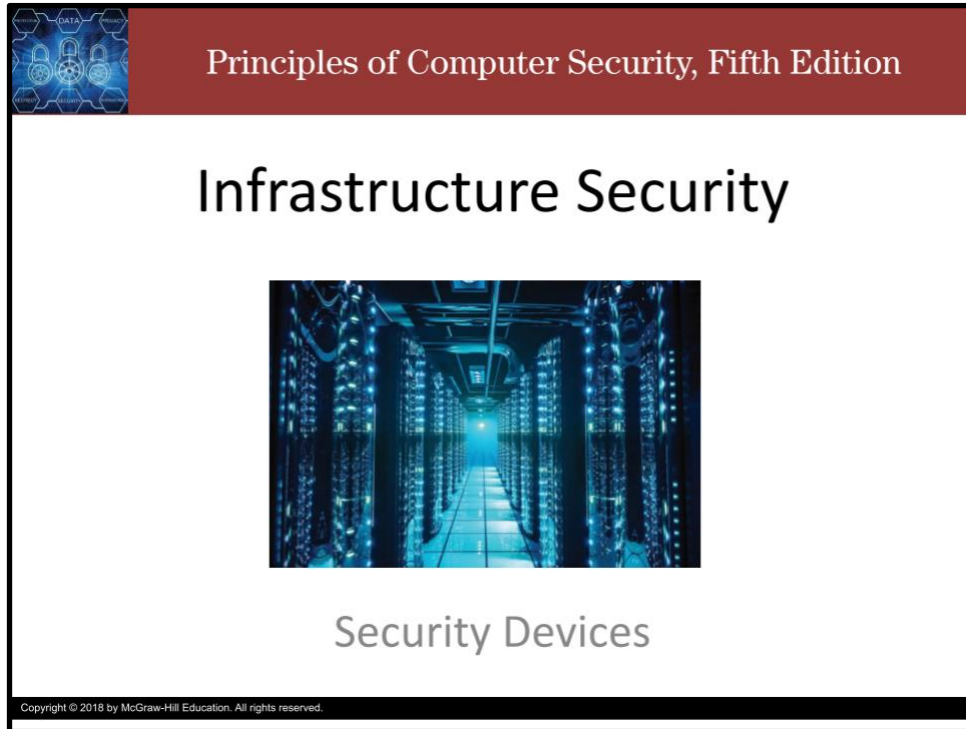
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care

Infrastructure Security: Security Devices


Slide 1



The image shows the cover of a book titled "Principles of Computer Security, Fifth Edition". The cover has a dark red header with the title in white serif font. Below the header, the main title "Infrastructure Security" is written in a large, black, sans-serif font. Underneath the title is a photograph of a server room with rows of server racks illuminated by blue lights. Below the photograph, the subtitle "Security Devices" is written in a smaller, grey, sans-serif font. In the bottom left corner of the cover, there is a small icon with the word "DATA" and some gears. At the very bottom of the cover, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Infrastructure Security




Security Devices

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we introduce network devices used to support network infrastructure security.

Slide 2



Principles of Computer Security, Fifth Edition

Security Devices


- There are a range of security devices that can be employed at the network layer to instantiate security functionality in the network layer.
- Devices can be used for intrusion detection, network access control, and a wide range of other security functions.
- Each device has a specific network function and plays a role in maintaining network infrastructure security.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There are a range of security devices that can be employed at the network layer to instantiate security functionality in the network layer. There are devices for intrusion detection, network access control, and a wide range of other security functions.

Each device has a specific network function and plays a role in maintaining network infrastructure security.

Slide 3



Principles of Computer Security, Fifth Edition

Intrusion Detection Systems (IDS)

- Designed to detect, log, and respond to unauthorized network or host use, both in real time and after the fact.
- Implemented using software.
 - In large networks or systems with significant traffic levels, dedicated hardware is typically required as well.
- Two categories:
 - Network-based systems and host-based systems


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Intrusion detection systems, or IDSs are designed to detect, log, and respond to unauthorized network or host use, both in real time and after the fact. These systems are implemented using software.

In large networks or systems with significant traffic levels, dedicated hardware is typically required as well.

IDSs can be divided into two categories: Network-based systems (for detecting intrusions into the network) and host-based systems (for detecting intrusions into an individual computer).

Slide 4



Principles of Computer Security, Fifth Edition

Network Monitoring/Diagnostic

- A **network operations center (NOC)** allows operators to observe and interact with the network, using the self-reporting and, in some cases, self-healing nature of network devices to ensure efficient network operation.
 - Software enables controllers at NOCs to measure the actual performance of network devices and make changes to the configuration and operation of devices remotely.
 - SNMP was developed to perform management, monitoring, and fault resolution across networks.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

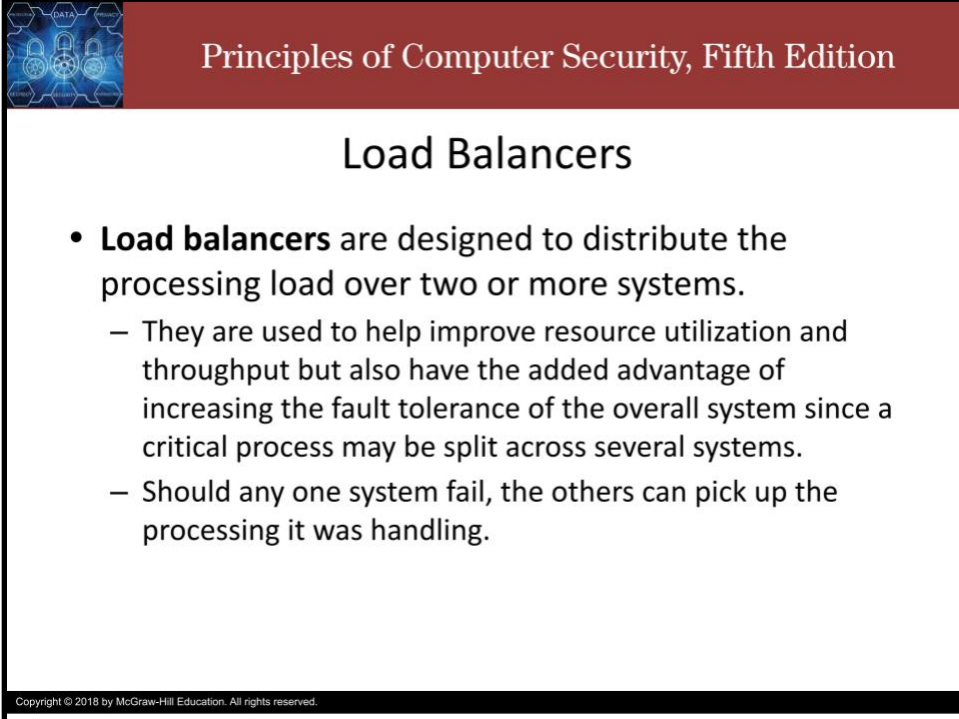
A computer network itself can be considered a large computer system, with performance and operating issues. Just as a computer needs management, monitoring, and fault resolution, so do networks. SNMP was developed to perform this function across networks. The idea is to enable a central monitoring and control center to maintain, configure, and repair network devices, such as switches and routers, as well as other network services, such as firewalls, IDSs, and remote access servers. SNMP has some security limitations, and many vendors have developed software solutions that sit on top of SNMP to provide better security and better management tool suites.

The concept of a **network operations center (NOC)** comes from the old phone company network days, when central monitoring centers monitored the health of the telephone network and provided interfaces for maintenance and management. This same concept works well with computer networks, and companies with midsize and larger networks employ the same philosophy. The NOC allows operators to observe and interact with the network, using the self-reporting and, in some cases, self-healing nature of network devices to ensure efficient network operation. Although generally a boring operation under normal conditions, when things start to go wrong, as in the case of a virus or worm attack, the NOC can become a busy and stressful place as operators attempt to return the system to full efficiency while not interrupting existing traffic. The operations of a NOC maybe subsumed in a network security operations center, NSOC, or a general-purpose security operations center, SOC.

SNMP is the main standard embraced by vendors to permit interoperability. Although SNMP has received a lot of security-related attention of late due to various security holes in its implementation, it is still an important part of a security solution associated with network infrastructure. Many useful tools have security issues; the key is to understand the limitations and to use the tools within correct boundaries to limit the risk associated with the vulnerabilities. Blind use of any technology will result in

increased risk, and SNMP is no exception. Proper planning, setup, and deployment can limit exposure to vulnerabilities. Continuous auditing and maintenance of systems with the latest patches is a necessary part of operations and is essential to maintaining a secure posture.

Slide 5



Principles of Computer Security, Fifth Edition

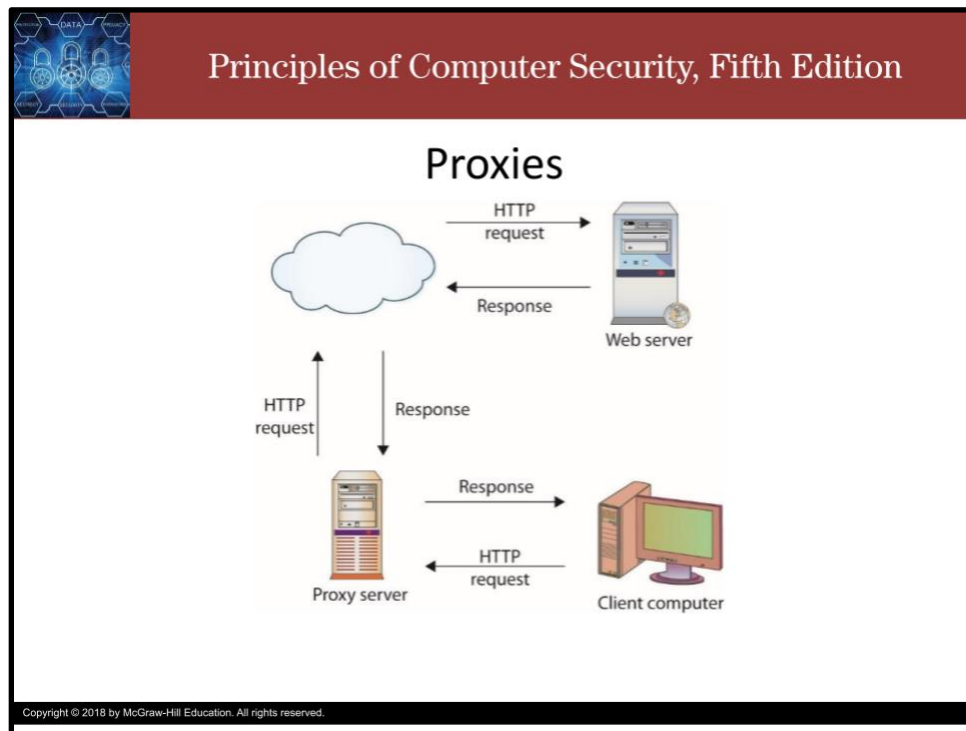
Load Balancers

- **Load balancers** are designed to distribute the processing load over two or more systems.
 - They are used to help improve resource utilization and throughput but also have the added advantage of increasing the fault tolerance of the overall system since a critical process may be split across several systems.
 - Should any one system fail, the others can pick up the processing it was handling.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Load balancers are designed to distribute the processing load over two or more systems. They are used to help improve resource utilization and throughput but also have the added advantage of increasing the fault tolerance of the overall system since a critical process may be split across several systems. Should any one system fail, the others can pick up the processing it was handling.

Slide 6




A **proxy server** (or simply proxy) can be used to filter out undesirable traffic and prevent employees from accessing potentially hostile web sites. Proxy servers can be completely transparent (gateways or tunneling proxies), or a proxy server can modify the client request before sending it on, or even serve the client's request without needing to contact the destination server. There are several major categories of proxy servers, such as anonymizing, caching, content-filtering, and web proxies.

Proxies serve to manage connections between systems, acting as relays for the traffic. Proxies can function at the circuit level, where they support multiple traffic types, or they can be application-level proxies, which are designed to relay specific application traffic. An HTTP proxy can manage an HTTP conversation as it understands the type and function of the content. Application-specific proxies can serve as security devices if they are programmed with specific rules designed to provide protection against undesired content.

From a security perspective, proxies are most useful in their ability to control and filter outbound requests. By limiting the types of content and web sites employees can access from corporate systems, many administrators hope to avoid loss of corporate data, hijacked systems, and infections from malicious web sites. Administrators also use proxies to enforce corporate Acceptable Use Policies and track use of corporate resources. Most proxies can be configured to either allow or require individual user authentication—this gives them the ability to log and control activity based on specific users or groups. For example, an organization might want to allow the human resources group to browse Facebook during business hours but not allow the rest of the organization to do so. Purely for hiring purposes, of course.

Slide 7




Principles of Computer Security, Fifth Edition

Web Security Gateways

- Some security vendors combine proxy functions with content-filtering functions to create a product called a **web security gateway**.
 - They are intended to address the security threats and pitfalls unique to web-based traffic.
- Web security gateways capabilities include:
 - Real-time malware protection
 - Content monitoring
 - Productivity monitoring
 - Data protection and compliance

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Some security vendors combine proxy functions with content-filtering functions to create a product called a **web security gateway**. Web security gateways are intended to address the security threats and pitfalls unique to web-based traffic. Web security gateways typically provide capabilities like real-time malware protection, content monitoring, productivity monitoring, and Data protection.



Principles of Computer Security, Fifth Edition


Internet Content Filters

- An **Internet content filter** protects a corporation from employees' viewing of inappropriate or illegal content at the workplace and the subsequent complications that occur when such viewing takes place.
- They filter undesirable content, such as pornography and malicious activity such as browser hijacking attempts or XSS attacks.
- Content-filtering systems face many challenges.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Content-filtering systems face many challenges, because the ever-changing Internet makes it difficult to maintain lists of undesirable sites. Terms used on a medical site can also be used on a pornographic site, making keyword filtering challenging; and determined users are always seeking ways to bypass proxy filters. To help administrators, most commercial content-filtering solutions provide an update service, much like IDS or antivirus products that updates keywords and undesirable sites automatically.

Slide 9



Principles of Computer Security, Fifth Edition

Data Loss Prevention

- **Data loss prevention (DLP)** refers to technology employed to detect and prevent transfers of data across an enterprise.
 - DLP technology can scan packets for specific data patterns.
 - DLP can be tuned to detect account numbers, secrets, specific markers, or files.
 - The primary challenge is the placement of the sensor.
 - The DLP sensor needs to be able observe the data, so if the channel is encrypted, DLP technology can be thwarted.

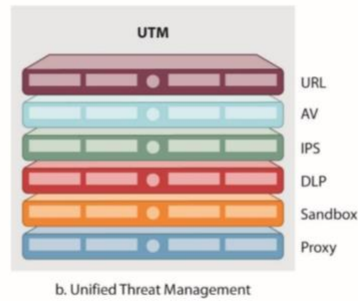
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Data loss prevention (DLP) refers to technology employed to detect and prevent transfers of data across an enterprise.

DLP technology can scan packets for specific data patterns. The primary challenge is the placement of the sensor. The DLP sensor needs to be able observe the data, so if the channel is encrypted, DLP technology can be thwarted.

Slide 10

Unified Threat Management



Copyright © 2018 by McGraw-Hill Education. All rights reserved.


A **unified threat management (UTM)** appliance is an “all-in-one” security appliances that combine multiple security functions into the same hardware appliance.

Most commonly these functions are firewall, IDS/IPS, and antivirus, although they can also include VPN capabilities, antispam, malicious web traffic filtering, antispysware, content filtering, traffic shaping, and so on.

A UTM simplifies the security activity as a single task, under a common software package for operations. This reduces the learning curve to a single tool rather than a collection of tools. A UTM solution can have better integration and efficiencies in handling network traffic and incidents than a collection of tools connected together.

This figure illustrates the advantages of UTM processing. Rather than processing elements in a linear fashion, as shown on top, the packets can be processed in a parallelized fashion for efficiency.

Slide 11



Principles of Computer Security, Fifth Edition

Attribution

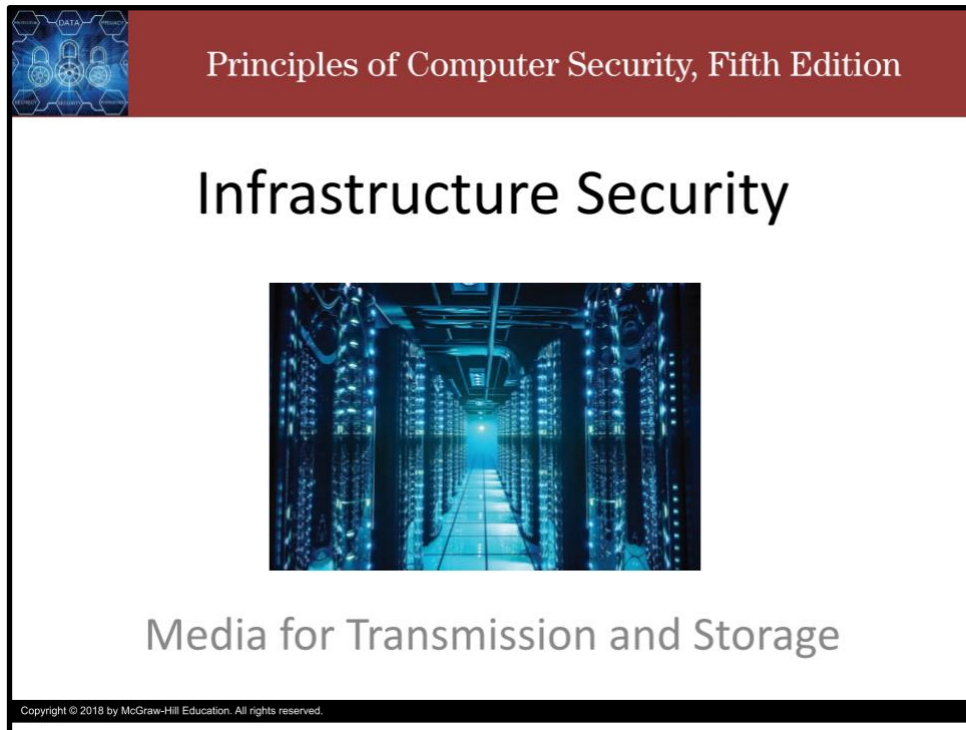
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.


Infrastructure Security: Media for Transmission and Storage

Slide 1



Principles of Computer Security, Fifth Edition

Infrastructure Security




Media for Transmission and Storage

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we introduce media used for data transmission and storage.

Slide 2



Principles of Computer Security, Fifth Edition


Media

- Four common methods are used to connect equipment at the physical layer:
 - Coaxial cable
 - Twisted-pair cable
 - Fiber-optics
 - Wireless

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


The base of communications between devices is the physical layer of the OSI model. This is the domain of the actual connection between devices, whether by wire, fiber, or by electromagnetic waves. The physical layer separates the definitions and protocols required to transmit the signal physically between boxes from higher-level protocols that deal with the details of the data itself. Four common methods are used to connect equipment at the physical layer: coaxial cable, twisted-pair cable, fiber-optics, and wireless.

Slide 3



Principles of Computer Security, Fifth Edition

Coaxial Cable



Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Coaxial cable is familiar to many households as a method of connecting televisions to VCRs or to satellite or cable services. It is used because of its high bandwidth and shielding capabilities. Compared to standard twisted pair lines such as telephone lines, coaxial cable, or “coax,” is much less prone to outside interference. It is also much more expensive to run, both from a cost-per-foot measure and from a cable-dimension measure. Coax costs much more per foot than standard twisted-pair wires and carries only a single circuit for a large wire diameter.

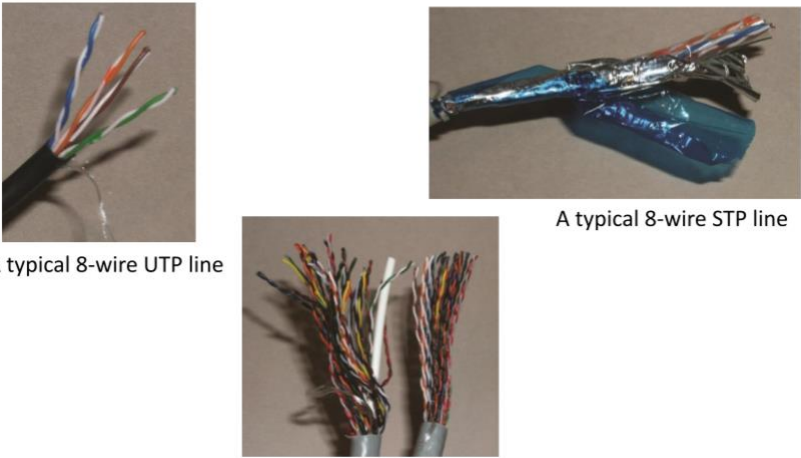
An original design specification for Ethernet connections, coax was used from machine to machine in early Ethernet implementations. The connectors were easy to use and ensured good connections, and the limited distance of most office LANs did not carry a large cost penalty. Today, almost all of this older Ethernet specification has been replaced by faster, cheaper twisted-pair alternatives, and the only place you’re likely to see coax in a data network is from the cable box to the cable modem.

Because of its physical nature, it is possible to drill a hole through the outer part of a coax cable and connect to the center connector. This is called a “vampire tap” and is an easy method to get access to the signal and data being transmitted.

Slide 4

Principles of Computer Security, Fifth Edition

Twisted Pair (STP/UTP)



A typical 8-wire UTP line

A typical 8-wire STP line

A bundle of UTP wires

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Twisted-pair wires have all but completely replaced coaxial cables in Ethernet networks. Twisted-pair wires use the same technology used by the phone company for the movement of electrical signals. Single pairs of twisted wires reduce electrical crosstalk and electromagnetic interference. Multiple groups of twisted pairs can then be bundled together in common groups and easily wired between devices.

Twisted pairs come in two types, shielded and unshielded. **Shielded twisted-pair (STP)** has a foil shield around the pairs to provide extra shielding from electromagnetic interference. **Unshielded twisted-pair (UTP)** relies on the twist to eliminate interference. UTP has a cost advantage over STP and is usually sufficient for connections, except in very noisy electrical areas.

Twisted-pair lines are categorized by the level of data transmission they can support, from Cat 3 which supports voice and 10-Mbps Ethernet, up to Cat 7 which supports 10-Gigabit Ethernet and higher.

The standard method for connecting twisted-pair cables is via an 8-pin connector, called an RJ-45 connector that looks like a standard phone jack connector but is slightly larger (if you've ever seen the end of an ethernet cable, you've seen an RJ45 connector). One nice aspect of twisted-pair cabling is that it's easy to splice and change connectors. Many a network administrator has made Ethernet cables from stock Cat-5 wire, two connectors, and a crimping tool. I actually wired my whole house for Ethernet this way, using Cat 5 cable I salvaged.

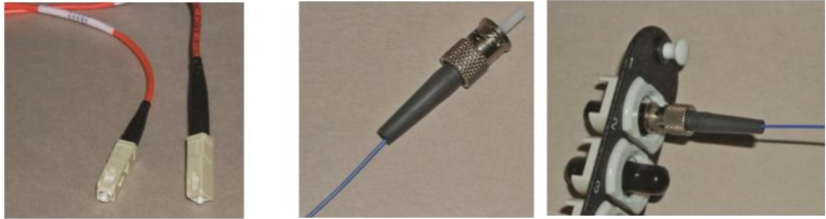
This ease of connection is also a security issue; because twisted-pair cables are easy to splice into, rogue connections for sniffing could be made without detection in cable runs. Both coax and fiber are much

more difficult to splice because each requires a tap to connect, and taps are easier to detect.

Slide 5

Principles of Computer Security, Fifth Edition

Fiber



A type of fiber terminator

A typical fiber-optic fiber, terminator, and connector block

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Fiber-optic cable uses beams of laser light to connect devices over a thin glass wire. One major advantage to fiber is its bandwidth, with transmission capabilities into the terabits per second range. Fiber optic cable is used to make high-speed connections between servers and is the backbone medium of the Internet and large networks.

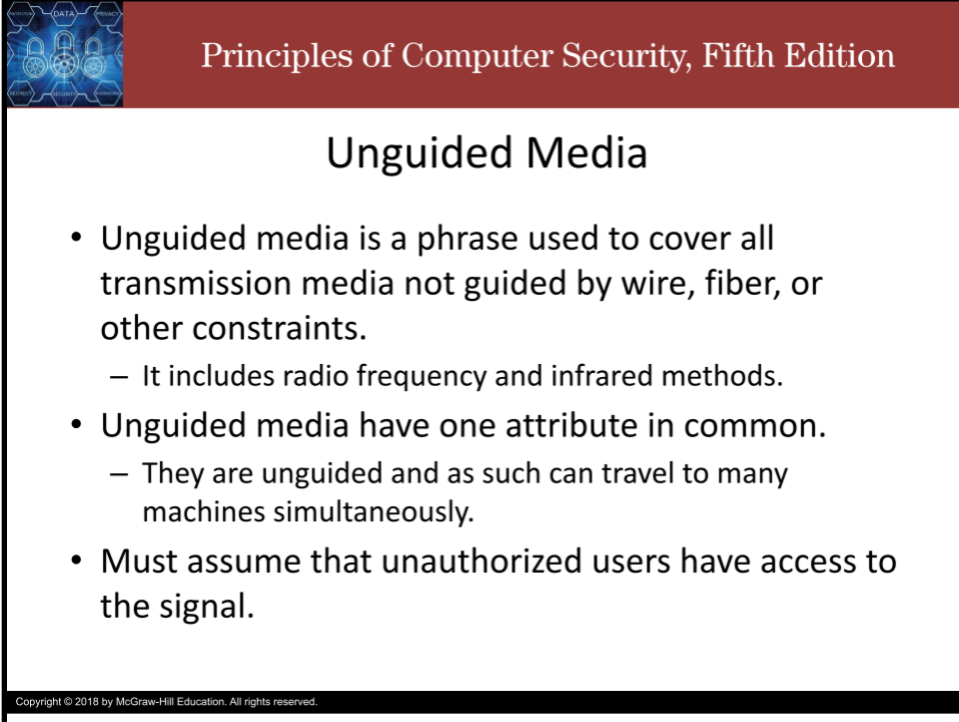
The length of runs of fiber can also be much longer, and the data capacity of fiber is much higher, than twisted pair cables. Fiber-optic technology is very expensive, though. The cables are expensive, but fiber is actually cheaper per megabit than competing wired technologies (assuming your other network devices also support those blazing speeds).

Connections to a fiber are difficult and expensive, and fiber is impossible to splice. Making the precise connection on the end of a fiber-optic line is a highly skilled job and is done by specially trained professionals who maintain a level of proficiency.

Splicing fiber is practically impossible; the solution is to add connectors and connect through a repeater. This adds to the security of fiber in that unauthorized connections are all but impossible to make. The high cost of connections to fiber and the higher cost of fiber per foot also make it less attractive for the

final mile in public networks where users are connected to the public switching systems. For this reason, Internet service providers use coax or twisted-pair to handle the “last mile”.

Slide 6



Principles of Computer Security, Fifth Edition

Unguided Media

- Unguided media is a phrase used to cover all transmission media not guided by wire, fiber, or other constraints.
 - It includes radio frequency and infrared methods.
- Unguided media have one attribute in common.
 - They are unguided and as such can travel to many machines simultaneously.
- Must assume that unauthorized users have access to the signal.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Unguided media is a phrase used to cover all transmission media not guided by wire, fiber, or other constraints. It includes radio frequency and infrared methods. Radio frequency waves are a common wireless communication method. Radio frequency is used for AM/FM radio, over-the-air TV, mobile phones, remote-controlled vehicles, and more.

Infrared (IR) is a band of electromagnetic energy just beyond the red end of the visible color spectrum. You are likely familiar with several devices which use IR, for example, IR has been used in remote-control devices for years.

Unguided media have one attribute in common: They can travel to many machines simultaneously. So, therefore, we must assume that unauthorized users have access to the signal and protect the data in transit accordingly.

Slide 7



Principles of Computer Security, Fifth Edition

Removable Media

- Moving storage media represents a security risk from a couple of angles.
 - The first is the potential loss of control over the data on the moving media.
 - Second is the risk of introducing unwanted items, such as a virus or a worm, when the media are attached back to a network.
 - Both of these issues can be remedied through policies and software.
 - The key is to ensure that the policies are enforced and the software is effective.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Moving storage media represents a security risk for at least two reasons.

The first is the potential loss of control over the data on the moving media.

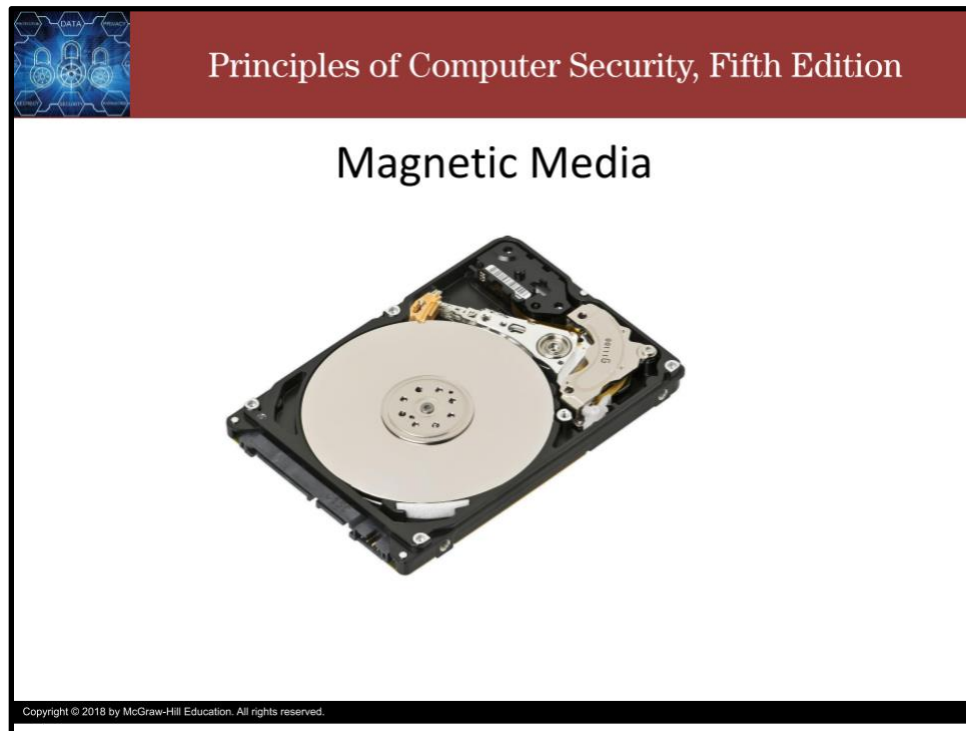
The second is the risk of introducing unwanted items, such as a virus or a worm, when the media are attached back to a network.

Both of these issues can be remedied through policies and software mechanisms.

The key is to ensure that the policies are effectively enforced by the software mechanisms.

The second risk of introducing malware into a network through a removable media device, can be mitigated by the physical mechanism of making it extremely difficult to connect removable devices, such as filling up ports with glue

Slide 8



Magnetic media store data through the rearrangement of magnetic particles on a nonmagnetic substrate. The most common form today is probably in hard drives. All these devices share some common characteristics: Each has sensitivity to external magnetic fields. They are also affected by high temperatures, as in fires, and by exposure to water.


Hard drives used to require large machines in mainframes. Now they are small enough to attach to mobile devices. The concepts remain the same among all of them: a spinning platter rotates the magnetic media beneath heads that read the patterns in the oxide coating. As drives have gotten smaller and rotation speeds have increased, the capacities have also grown. Today gigabytes of data can be stored in a device slightly larger than a bottle cap. Portable hard drives in the 1TB to 3TB range are now available and affordable.

One of the security controls available to help protect the confidentiality of the data is full drive encryption built into the drive hardware. Using a key that is controlled, through a Trusted Platform Module (TPM) interface for instance, this technology protects the data if the drive itself is lost or stolen. This may not be important if a thief takes the whole PC, but in larger storage environments, drives are placed in separate boxes and remotely accessed. In the specific case of notebook machines, this layer can be tied to smart card interfaces to provide more security. As this is built into the controller, encryption protocols such as Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) can be performed at full drive speed.

Slide 9

Principles of Computer Security, Fifth Edition

Optical Media



Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Optical media involve the use of a laser to read data stored on a physical device. A laser picks up deformities embedded in the media that contain the information. As with magnetic media, optical media can be read-write, although the read-only version is still more common.


There are 3 common optical media in use today: CDs, DVDs, and Blu-Ray discs. I think CDs are likely not long for this world, and DVDs won't be far behind. Even Blu-ray will eventually become obsolete.

CDs can hold up to 800MB of data. DVDs can hold 4.7 GB in a single layer, or 8.5 GB in a dual layer. Blu-ray discs can hold up to 128 GB in four layers. The transfer speed of Blu-ray, 4.5MBps up to 72MBps, is much higher than that of DVD systems, but only matches or slightly exceeds that of hard disk drives.

Slide 10

Principles of Computer Security, Fifth Edition

Electronic Media



SD, microSD, and CompactFlash cards

128GB USB 3.0 memory stick

512GB solid-state half-height minicard

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The latest form of removable media is electronic memory. Electronic circuits of static memory, which can retain data even without power, fill a niche where high density and small size are needed.


These memory devices range from small card-like devices, of which microSD cards are smaller than dimes and hold 2GB, to USB sticks that hold up to 2TB.

With the rise of solid-state memory technologies came also a solid-state “hard drive” to compete with and often replace (but also complement) magnetic hard disk drives.

With electronic media, there are no moving parts to wear out or fail and they have vastly superior performance specifications compared to optical and magnetic media.

Electronic media, like flash drives and solid-state hard drives, can have data transfers rates in the hundreds or thousands of MBps.

Slide 11



Principles of Computer Security, Fifth Edition

Attribution

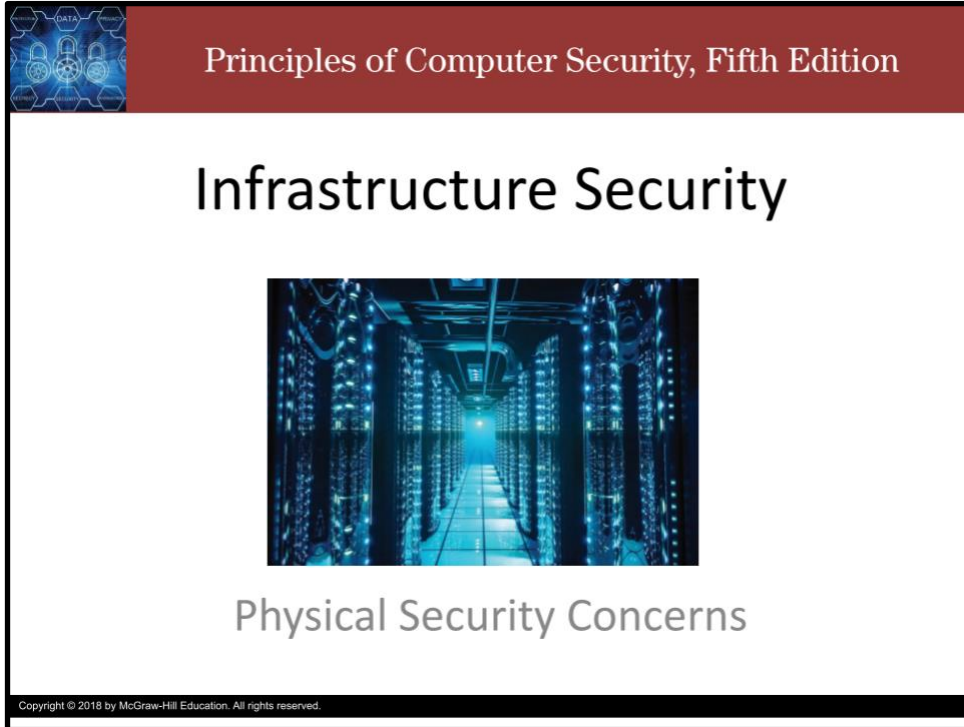
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Infrastructure Security: Physical Security Concerns


Slide 1



The image shows the cover of the book "Principles of Computer Security, Fifth Edition". The top left corner features a blue graphic with icons for "DATA", "SECURITY", and "NETWORK". The title "Principles of Computer Security, Fifth Edition" is written in white on a dark red background. Below this, the main title "Infrastructure Security" is displayed in large black font. A central photograph shows a perspective view of a server room with rows of racks illuminated by blue lights. Below the photo, the subtitle "Physical Security Concerns" is written in a smaller black font. At the bottom left, a small copyright notice reads "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy! In this video, we mention some physical security concerns for network infrastructure.

Slide 2



Principles of Computer Security, Fifth Edition

Physical Security Concerns

- The primary security concern for a system administrator has to be preventing physical access to a server by an unauthorized individual.
- One of the administrator's next major concerns should be preventing unfettered access to a network connection.
- Preventing such access is costly, yet the cost of replacing a server because of theft is also costly.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The primary security concern for a system administrator has to be preventing physical access to a server by an unauthorized individual.

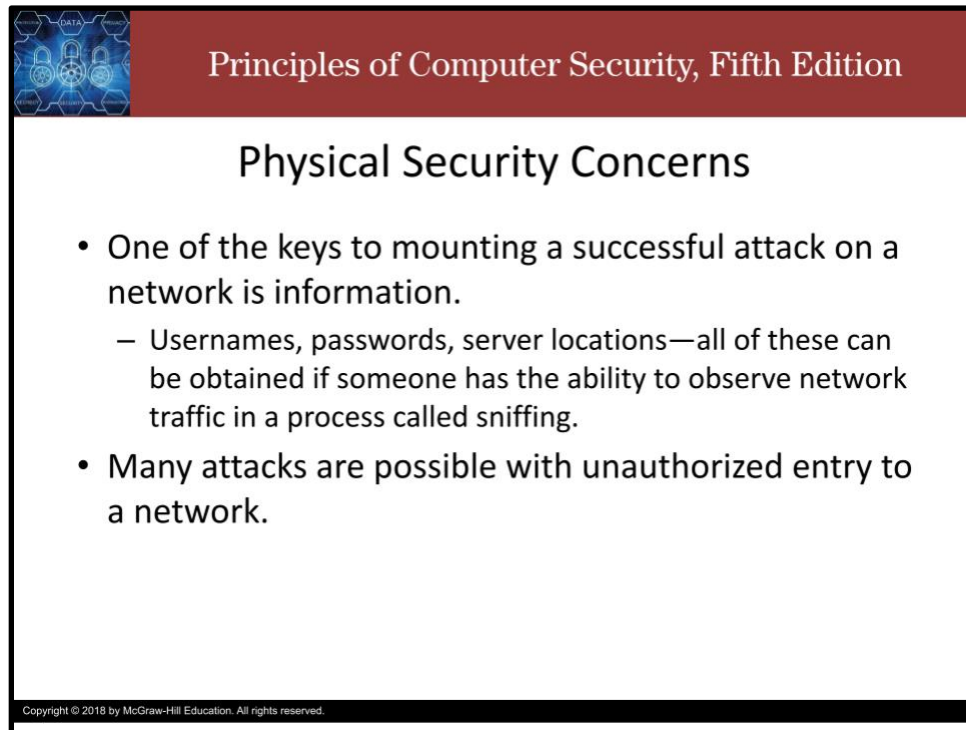
Such access will almost always spell disaster, for with direct access and the correct tools, any system can be infiltrated.

One of the administrator's next major concerns should be preventing unfettered access to a network connection.

Access to switches and routers is almost as bad as direct access to a server, and access to network connections would rank third in terms of worst-case scenarios.

Preventing such access is costly, yet the cost of replacing a server because of theft is also costly.

Slide 3



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. To the left of the header is a decorative graphic with blue and white icons representing data, locks, and network connectivity. The main content area is white with a black border. The title "Physical Security Concerns" is centered in a large, bold, black font. Below the title is a bulleted list with two main points and one sub-point. The first point is "One of the keys to mounting a successful attack on a network is information." followed by a sub-point: "– Usernames, passwords, server locations—all of these can be obtained if someone has the ability to observe network traffic in a process called sniffing." The second point is "Many attacks are possible with unauthorized entry to a network." At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Physical Security Concerns

- One of the keys to mounting a successful attack on a network is information.
 - Usernames, passwords, server locations—all of these can be obtained if someone has the ability to observe network traffic in a process called sniffing.
- Many attacks are possible with unauthorized entry to a network.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A balanced approach is the most sensible approach when addressing physical security, and this applies to transmission media as well.

Keeping network switch rooms secure and cable runs secure seems obvious, but cases of using janitorial closets for this vital business purpose abound.


One of the keys to mounting a successful attack on a network is information.

Usernames, passwords, server locations—all of these can be obtained if someone has the ability to sniff network traffic

A sniffer can record all the network traffic, and this data can be mined for accounts, passwords, and traffic content, all of which can be useful to an unauthorized user. One starting point for many intrusions is the insertion of an unauthorized sniffer into the network, with the fruits of its labors driving the remaining unauthorized activities. Many attacks are possible with unauthorized entry to a network, such as:

Inserting a node and functionality that is not authorized on the network, such as a sniffer device or unauthorized wireless access point, modifying firewall security policies, modifying access control lists for firewalls, switches, or routers, and modifying network devices to echo traffic to an external node.

Slide 4



Principles of Computer Security, Fifth Edition

Physical Security Concerns


- Limiting physical access is difficult and essential.
- Essential to prevent unauthorized contact with network equipment.
- Use a firewall with an authentication system or establish a VPN to ensure that unauthorized traffic does not enter your network through a wireless access point.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Network devices and transmission media become targets because they are dispersed throughout an organization, and physical security of many dispersed items can be difficult to manage. The least level of skill is still more than sufficient to accomplish unauthorized entry into a network if physical access to the network signals is allowed. This is one factor driving many organizations to use fiber-optics, for these cables are much more difficult to tap. Although many tricks can be employed with switches and VLANs to increase security, it is still essential that you prevent unauthorized contact with the network equipment.

Wireless networks make the intruder's task even easier, as they take the network to the users, authorized or not. A technique called war-driving involves using a laptop and software to find wireless networks from outside the premises. A typical use of war-driving is to locate a wireless network with poor (or no) security and obtain free Internet access, but other uses can be more devastating. A simple solution is to place a firewall between the wireless access point and the rest of the network and authenticate users before allowing entry. Business users use VPN technology to secure their connection to the Internet and other resources, and home users can do the same thing to prevent neighbors from "sharing" their Internet connections. To ensure that unauthorized traffic does not enter your network through a wireless access point, you must either use a firewall with an authentication system or establish a VPN.

Slide 5



Principles of Computer Security, Fifth Edition

Attribution

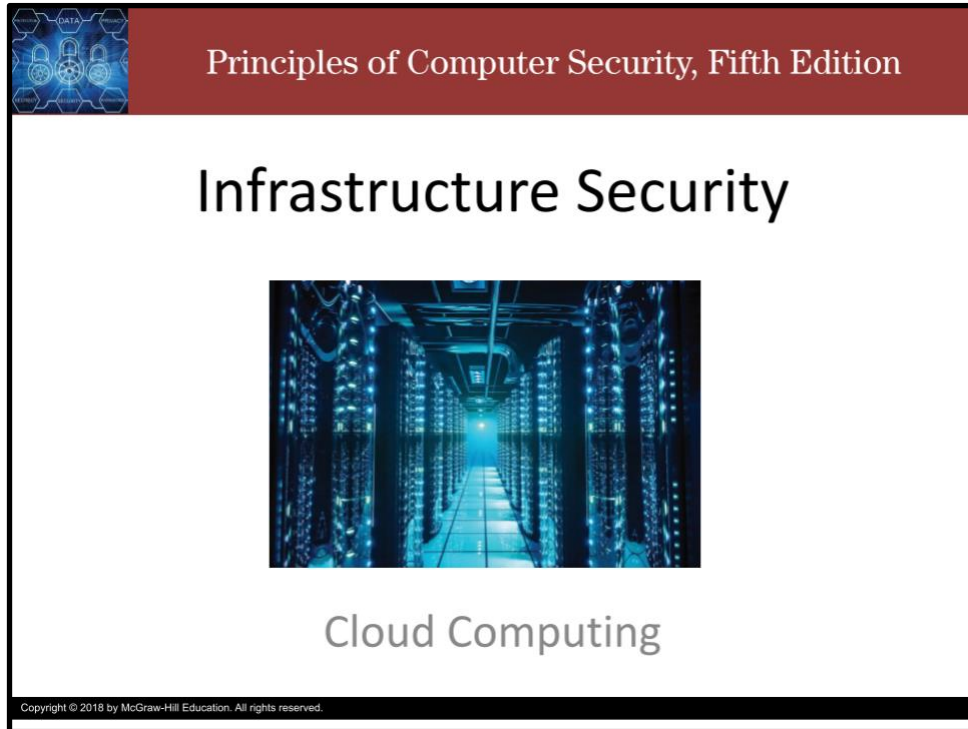
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Infrastructure Security: Cloud Computing


Slide 1



The image shows the cover of a book titled "Principles of Computer Security, Fifth Edition". The cover has a dark red header with the title in white. Below the header, the main title "Infrastructure Security" is written in a large, black, sans-serif font. Underneath the title is a photograph of a server room with rows of server racks illuminated by blue lights. Below the photograph, the words "Cloud Computing" are written in a smaller, grey, sans-serif font. In the top left corner of the cover, there is a small graphic with the word "DATA" and several padlock icons. At the very bottom of the cover, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Infrastructure Security




Cloud Computing

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we introduce cloud computing.

Slide 2



Principles of Computer Security, Fifth Edition

Cloud Computing

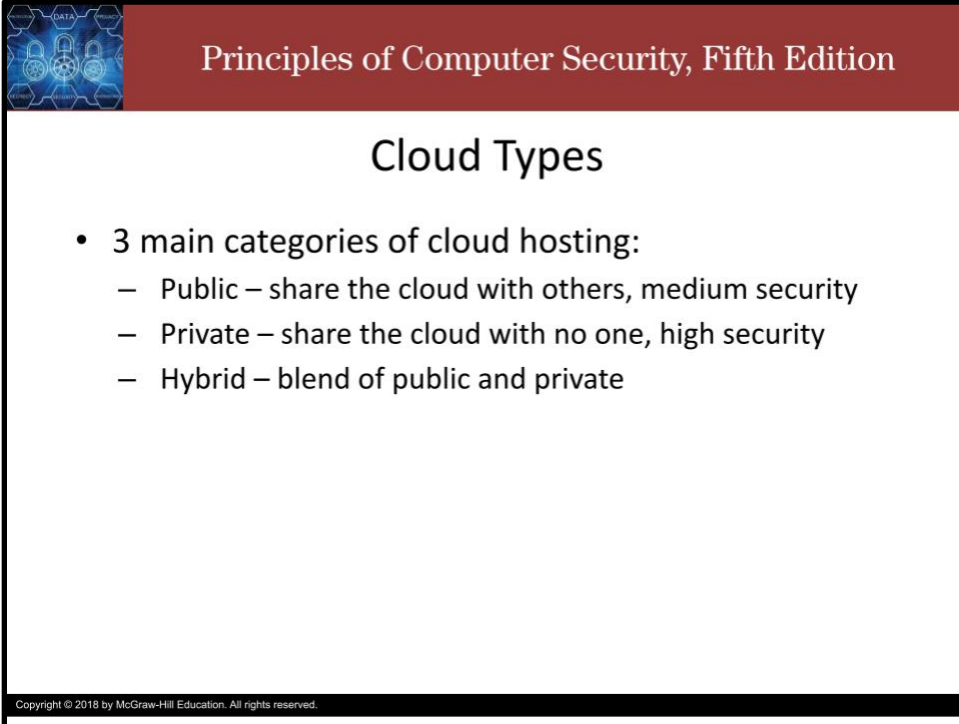
- Computer services provided over a network.
 - Computing, storage, applications, and services
 - Transparent to the end user.
- Security is a challenge
 - How to allow data outside the enterprise, but still maintain control?
 - Encryption

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Cloud computing is a common term used to describe computer services provided over a network. This includes computing, storage, applications, and services that are offered via the Internet Protocol. One of the characteristics of cloud computing is transparency to the end user.

Security is a particular challenge when data and computation are handled by a remote party, as in cloud computing. The specific challenge is how does one allow data outside their enterprise and yet remain in control over how the data is used, and the common answer is encryption. By properly encrypting data before it leaves the enterprise, external storage can still be performed securely.

Slide 3



Principles of Computer Security, Fifth Edition

Cloud Types

- 3 main categories of cloud hosting:
 - Public – share the cloud with others, medium security
 - Private – share the cloud with no one, high security
 - Hybrid – blend of public and private

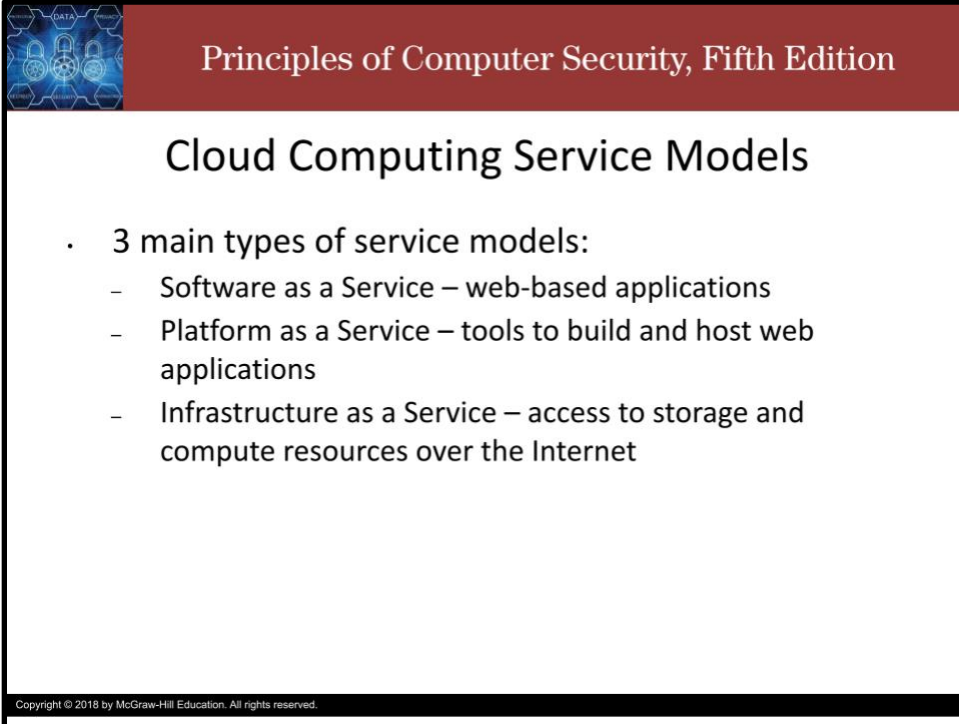
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Depending on the size and particular needs of an organization, there are three main categories of cloud hosting: public, private, and hybrid. The term public cloud refers to cloud service rendered over a system that is open for public use. In most cases, there is little operational difference between public and private cloud architectures, but the security ramifications can be substantial. Although public cloud services will separate users with security restrictions, the depth and level of these restrictions, by definition, will be significantly less in a public cloud.

If your organization is highly sensitive to sharing resources, you may wish to consider the use of a private cloud. Private clouds are essentially reserved resources used only for your organization—your own little cloud within the cloud. This service will be considerably more expensive, but it should also carry less exposure and should enable your organization to better define the security, processing, and handling of data that occurs within your cloud.

A hybrid cloud structure is one where elements are combined from public and private cloud structures. When examining a hybrid structure, you need to remain cognizant that operationally these differing environments may not actually be joined, but rather used together. Sensitive information can be stored in the private cloud and public-facing information, such as the organizations public website, can be stored in the public cloud.

Slide 4



Principles of Computer Security, Fifth Edition

Cloud Computing Service Models

- 3 main types of service models:
 - Software as a Service – web-based applications
 - Platform as a Service – tools to build and host web applications
 - Infrastructure as a Service – access to storage and compute resources over the Internet

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There are three main types of cloud computing services. They are sometimes called the cloud computing stack because they build on top of one another.

Software as a Service (or SaaS) is the offering of software to end users from within the cloud. Rather than installing software on client machines, SaaS acts as software on demand where the software runs from the cloud. This has several advantages, as updates are often seamless to end users and integration between components is enhanced.

Platform as a Service (or PaaS) is the offering of a computing platform in the cloud. Multiple sets of software, working together to provide services, such as database services, can be delivered via the cloud as a platform.

Infrastructure as a Service (or IaaS) is renting IT infrastructure in the cloud. Rather than building data centers, IaaS allows firms to contract for utility computing or storage as needed.

Principles of Computer Security, Fifth Edition

Attribution

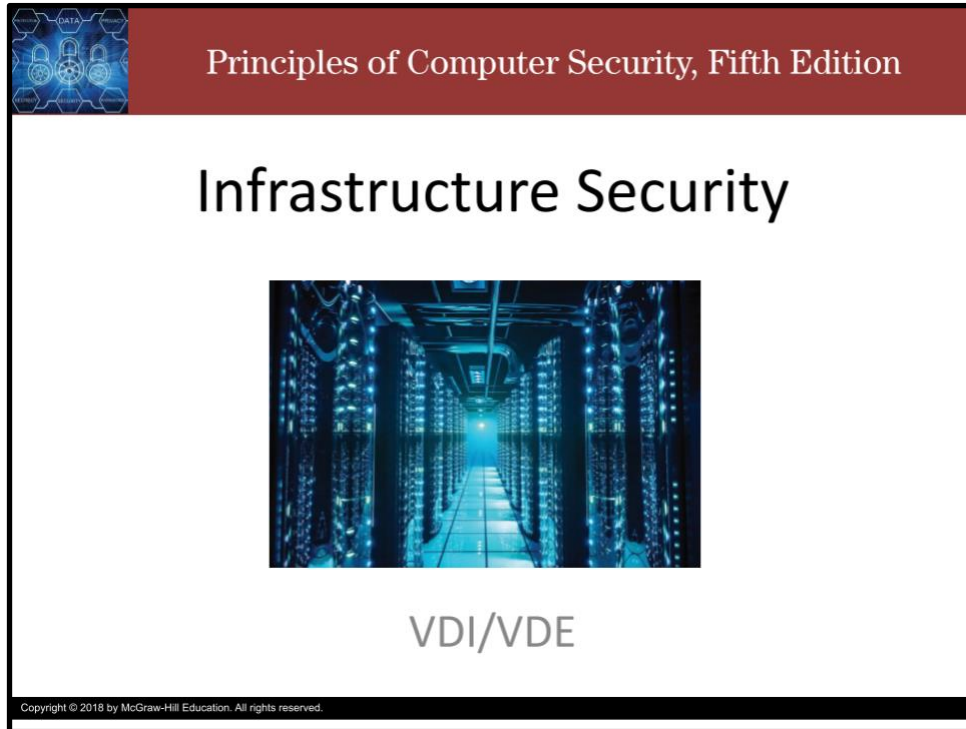
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Infrastructure Security: VDI/VDE


Slide 1



The image shows a book cover with a dark red header. The header contains the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the title "Infrastructure Security" is written in a large, black, sans-serif font. Underneath the title is a photograph of a server room with rows of server racks illuminated by blue light. Below the photograph, the text "VDI/VDE" is written in a grey, sans-serif font. In the bottom left corner of the cover, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Infrastructure Security




VDI/VDE

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we introduce VDI and VDE.

Slide 2



Principles of Computer Security, Fifth Edition

VDI and VDE

- **Virtual Desktop Infrastructure**
- **Virtual Desktop Environment**
- **Advantages to this desktop environment:**
 - From a user perspective, their “machine” and all of its data are persisted in the server environment.
 - Computing requirements at the edge point are considerably lower and can be performed on older machines.
 - Users can utilize a wide range of machines to get their work finished.
 - Better security because there is very little to compromise if a device is lost.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


Virtual desktop infrastructure (VDI) and virtual desktop environment (VDE) are terms used to describe the hosting of a desktop environment on a central server.

There are several advantages to this sort of desktop environment. From a user perspective, their “machine” and all of its data persist in the server environment, so they can move between machines and always have their data right where they need it.

Computing requirements at the edge point are considerably lower and can be performed on older machines and a wide variety of devices, including mobile phones.

Confidentiality is supported because there is very little to compromise if a device is lost.

Slide 3



Principles of Computer Security, Fifth Edition

Attribution

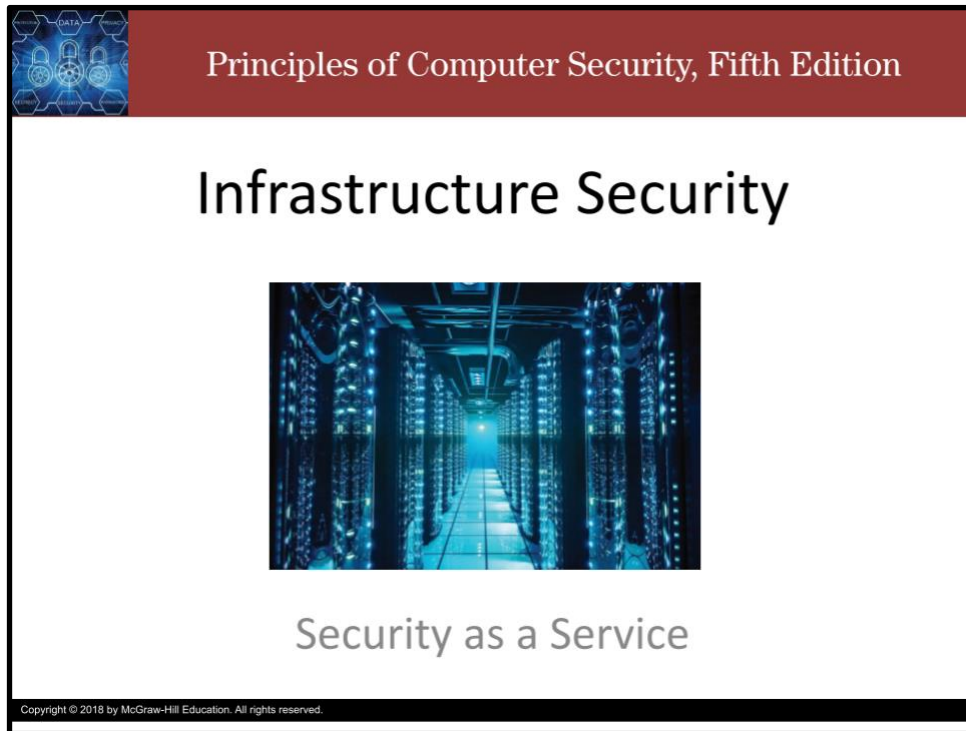
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Infrastructure Security: Security as a Service


Slide 1



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the title "Infrastructure Security" is centered in a large, black, sans-serif font. Underneath the title is a photograph of a server room with rows of server racks illuminated by blue lights. Below the photograph, the subtitle "Security as a Service" is centered in a smaller, grey, sans-serif font. In the bottom left corner of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

Infrastructure Security




Security as a Service

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we introduce security as a service.

Slide 2



Principles of Computer Security, Fifth Edition

Security as a Service


- Security as a Service is the outsourcing of security functions to a vendor that has advantages in scale, costs, or speed.
- Different security vendors offer different specializations
- Depending on architecture, needs, and scale, these third-party vendors can oftentimes offer a compelling economic advantage for part of a security solution.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Security as a Service is the outsourcing of security functions to a vendor that has advantages in scale, costs, or speed.

Different security vendors offer different specializations and, depending on architecture, needs, and scale, these third-party vendors can sometimes offer a compelling economic advantage for part of a security solution.

Slide 3



Principles of Computer Security, Fifth Edition


Cloud Access Security Broker

- Integrated suites of tools or services offered as SECaaS or 3rd party MSSPs focused on cloud security.
- CASB vendors provide security services designed to protect cloud infrastructure and data.
- CASBs act as security policy enforcement points between cloud service providers and their customers.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Cloud access security brokers or CASBs, are integrated suites of tools or services offered as Security as a Service, or third-party managed security service providers (MSSPs), focused on cloud security. CASB vendors provide a range of security services designed to protect cloud infrastructure and data. CASBs act as security policy enforcement points between cloud service providers and their customers to enact enterprise security policies as the cloud based resources are utilized.

Slide 4



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.